ENTRUST CERTIFICATE SERVICES

PRIVACY STATEMENT

Contents

Entrust Certificate Services 3

Entrust Certificate Services (ECS) 3

Description 3

Personal Data Collection and Processing 3

Retention Period 4

Use of Sub-Processors 4

International Data Transfers 4

Data Protection Measures 4

Data Privacy Rights 4

Amendments to this Privacy Statement 4

Contact Information 4

Certificate Services Products 5

Document Signing Certificates 5

Public Code Signing 5

Public Key Infrastructure as a Service (PKIaaS) 6

Public TLS/SSL 6

Public SMIME 6

Qualified Certificates 6

Remote Signing Service (RSS) 7

Signing Automation Service (SAS) 7

Verified Mark Certificates (VMC) 8

Entrust Certificate Services

Last Updated: November 25, 2021

Entrust Certificate Services (ECS)

This product privacy notice describes how Entrust Certificate Services (ECS) collects and processes personal data pursuant to applicable data privacy laws.

Description

ECS is a web-based certificate lifecycle management platform that helps you manage all of your digital certificates, from both Entrust and other Certification Authorities. It provides access to a host of tools generating detailed reports that help users to improve uptime, avoid security lapses and preserve brand reputation. ECS provides web-based access to technical insights, status updates, and website scanning for end-to-end lifecycle management of all of your digital certificates.

Personal Data Collection and Processing

Entrust's ECS collects the following data for authorized representatives of our Customers:

Personal Data Type	**Purpose for Processing**
Company Address	Public Trust Compliance/Account management
Company/Organization	Public Trust Compliance/Account management
Email Address	User authentication
IP Address	Security
Job Title/Position	Public Trust Compliance
Name	Public Trust Compliance
Password	User authentication
Phone Number	Public Trust Compliance
Security Questions and Answers	User authentication
Username	User authentication

Retention Period

All personal data collected by ECS is retained in accordance with the terms set forth in Customer contracts.

Use of Sub-Processors

For the current list of sub-processors, visit https://www.entrust.com/legal-compliance/privacy/sub-processors.

International Data Transfers

Entrust's certificate products make use of various sub-processors and data centers. To the extent that Customers are located in a different country than the sub-processor used for identification verification, SMS authentication, provision of one-time passwords (OTPs), or data hosting, there may be cross-border transfers of personal data. Any cross-border transfers of personal data are made in accordance with relevant data privacy law requirements (e.g., the Standard Contractual Clauses for EU personal data transferred out of the EU).

Data Protection Measures

For more information on how Entrust processes personal data collected by this product, please refer to Schedule 2, Appendix 2 of our standard customer data processing agreement (DPA) found here.

Data Privacy Rights

The Customer is the data controller for all personal data collected by ECS. Entrust Corporation, as the data processor, will assist the Customer, to the extent reasonable and practicable, in responding to verified data subject access requests the Customer receives with respect to ECS.

Amendments to this Privacy Statement

We reserve the right to amend this Product Privacy Statement from time to time as our business, laws, regulations and industry standards evolve. Any changes are effective immediately following the posting of such changes to https://www.entrust.com/legal-compliance/data-privacy/product-privacy-notices. We encourage you to review this statement from time to time to stay informed.

Contact Information

For questions about this product privacy notice, please contact privacy@entrust.com. For Entrust Corporation's general privacy notice, please click here.

Certificate Services Products

Document Signing Certificates

Entrust Document Signing Certificates enable organizations to establish trust of electronically transmitted documents and digitally sign Adobe and Microsoft Office documents with confidence. Enabled by proven public key infrastructure (PKI) technology, digital signatures are widely recognized as a best practice for providing digital verification of electronic transmissions. Digital signatures provide “non-repudiation,” the ability to identify the author and verify that the document has not been changed since it was digitally signed. Real-time assurance verifies authenticity throughout the document’s lifetime. Organizations can also use Document Signing Certificates to authenticate sensitive documents requiring multiple signatures .

Additional Personal Data Collected:

Some Document Signing Certificates may also require date of birth and national identification numbers. Further, Document Signing Certificates may require collection and storage of a copy of the subscriber’s identification document, a picture of their face along with a short video from the ID verification session. The purpose for processing this data is identity verification. Biometric data will only be processed in case of identity verification via video.

Mobile Device Certificates

Entrust Mobile Device Certificates provide a cloud-based solution for authenticating mobile devices and providing secure access to corporate systems without deploying an on-premises PKI. With Entrust Mobile Device Certificates, Customers can easily provision and manage digital identities and devices in BYOD environments, giving their users a frictionless experience while meeting internal security requirements.

Additional Personal Data Collected:

Entrust Mobile Device Certificates require end-users to select a Device Name and a Common Name. These two names do not necessarily contain personal data, but could depending on what the end-user populates the custom field with. The Device Name is not publicly viewable, but the Common Name appears in the certificate.

Public Code Signing

Entrust Public Code Signing Certificates authenticate the publisher’s identity and verify that the digitally signed executables and scripts have not been tampered with since signing. This assures Customers that the signed software will be downloaded from the internet as the developer intended. Signed certificates help software publishers establish trust with their customers, preventing unverified software from being installed on corporate devices. Users feel confident knowing that the publisher was verified by Entrust, a WebTrust-accredited certification authority (CA).

Public Key Infrastructure as a Service (PKIaaS)

Entrust PKIaaS provides cloud-based, highly scalable, PKI that is backed by Entrust nShield HSM clusters hosted in Entrust data centers. PKIaaS provides an agile PKI backend to applications that require privately trusted certificates, such as mobile device management, user authentication, IoT and DevOps.

Public TLS/SSL

Entrust TLS/SSL Certificates provide validated identity and encryption to secure websites, users, and data. The use of non-Fully Qualified Domain Names (FQDNs) in publicly trusted certificates ceased on November 1, 2015, and existing certificates containing non-FQDNs were revoked by all public certification authorities by October 1, 2016. To help simplify this change, Entrust introduced Private SSL Certificates that provide organizations with an easy and affordable method for the continued use of non-registered domain names.

Public SMIME

Entrust SMIME Certificates provide a simple way to reduce the possibility of critical data loss and attacks coming from email. The authentication and end-to-end encryption of internal/external emails, together with a fully automated deployment of S/MIME certificates and lifecycle management at scale, is one of many capabilities that makes our solution stand out from traditional solutions. Entrust SMIME Certificates comply with various confidentiality regulations related to healthcare, education, government, military, financial, and other consumer sectors.

Qualified Certificates

Qualified Certificates from Entrust provide secure, authenticated communications that comply with European Union (EU) data security standards and regulations, including the Revised Payment Services Directive (PSD2).

Qualified Certificates can only be issued by a Qualified Trust Service Provider (QTSP) recognized under electronic identification and trust services (eIDAS). Entrust Europe is recognized across all EU and European Economic Area (EEA) countries as a QTSP and has undergone the appropriate eIDAS conformity assessments in order to be able to provide Qualified Certificates for Website Authentication. View Entrust Europe on the EU Trust List.

Additional Personal Data Collected:

Qualified Certificates may also require collection and storage of a copy of the subscriber's identification document, a picture of their face, along with a short video from the ID verification session. The purpose for processing this data is identity verification. Biometric data will only be processed in case of identity verification via video.

Remote Signing Service (RSS)

Entrust Digital Signing as a Service helps companies and institutions to establish high assurance digital signatures and company seals without the need for hardware maintenance or crypto expertise though a web application programming interface (API). Entrust Remote Signing Service is an extension of the above that enables employees to apply digital signatures on documents with their signing keys, centrally managed in a remote service.

Signing keys are centrally protected within a Hardware Security Module (HSM), and document signatures are approved remotely by users from their device, without the need for a hardware or software token.

The platform provides advanced and qualified signatures as defined by eIDAS. It is based on European Telecommunications Standards Institute (ETSI) and the European Committee for Standardization (CEN) standards, which guarantee a very high level of trust and a broad interoperability with the industry products that require digital signatures. The user onboarding and signing process is transparent, does not require specific knowledge, and can be done from any device.

Additional Personal Data Collected:

RSS may also require collection and storage of a copy of the subscriber's identification document, a picture of their face, along with a short video from the ID verification session. The purpose for processing this data is identity verification. Biometric data will only be processed in case of identity verification via video.

Signing Automation Service (SAS)

With Entrust Signing Automation Service, Customers get all the benefits of a company seal on their documents without the complexity of hardware management and the risks of manual signing. Authorship, integrity, and nonrepudiation for all customer documents is achieved by integrating this cloud-based service into the customer applications with Entrust signing automation client. Customers get globally recognized document signing certificates plus timestamping and Online Certificate Status Protocol (OCSP) services all backed by cloud-based HSMs from our data centers.

Additional Personal Data Collected:

Signing Automation Service also requires validation of a representative of the organization, which includes collecting and storing a copy of the representative's identification document, a picture of their face, along with a short video from the ID verification session. The purpose for processing this data is identity verification. Biometric data will only be processed in case of identity verification via video.

Verified Mark Certificates (VMC)

Verified Mark Certificates allow brands to show their registered brand logo alongside email communications.

Entrust, in collaboration with AuthIndicators Working Group, developed a method for standardizing the appearance of verified logos alongside received emails. The method includes the use of a Verified Mark Certificate, which verifies the brand's logo. Brand Indicators for Message Identification (BIMI) is the standards body for the combined technology that enables VMC issuance.

Additional Personal Data Collected:

Verified Mark Certificates also require collection and storage of a copy of the subscriber's identification document, a picture of their face, along with a short video from the ID verification session. The purpose for processing this data is identity verification. Biometric data will only be processed in case of identity verification via video.